Claims:

1. A communication system using quantum cryptography, comprising subscriber stations (1.i, 2.i) which are connected to quantum channels (3) and quantum-cryptographic devices (10, 11) which are associated with the quantum channels for generating a quantum key, characterized in that several interconnected switching stations (1, 2) are provided to which the subscriber stations (1.i, 2.i) are connected via the quantum channels (3) for generating a respective temporary quantum key.

2. A communication system according to claim 1, characterized in that the switching stations (1, 2) contain a source of photons (10) as quantum-cryptographic device as well as also a photon detector (11), in case interlaced photons are used.

3. A communication system according to claim 2, characterized in that the subscriber stations (1.i, 2.i)merely contain a photon detection device (11').

4. A communication system according to any one of

claims 1 to 3, characterized in that switching stations (1, 2, 6', 7') are interconnected at least partially in the form of point-to-point links.

5. A communication system according to any one of claims 1 to 3, characterized in that the switching stations (1, 2, 6-9) at least partially are hierarchically interconnected.

6. A communication system according to any one of claims 1 to 5, characterized in that the subscriber stations (1.i, 2.i) communicate via public lines (4)using the quantum key generated via the switching stations (1, 2).

7. A communication system according to any one of claims 1 to 6, characterized in that the subscriber stations (1.1, 2.1) involved in the desired communication generate a separate key bit sequence with their associated switching station (1, 2) via the quantum channel (3) after a request for a communication has been transmitted via the respective switching station (1, 2).

8. A communication system according to claim 7, characterized in that the switching station (2) associated with the called subscriber station (2.1) generates a third key bit sequence from the key bit sequences generated via the quantum channels (3), and transmits this third key bit sequence to the called subscriber station (2.1) which, using the key bit sequence known to it and generated by it together with the associated switching station, from this third key bit sequence generates the key bit sequence generated on the part of the calling subscriber station (1.1) which then finally is used as a mutual key for the communication between the subscriber stations (1.1, 2.1).

9. A communication system according to any one of claims 1 to 8, characterized in that when ending the communication, the quantum key generated for this communication is discarded.

10. A communication system according to any one of claims 1 to 9, characterized in that the generated quantum key is checked for its freedom from interference, and in that as a consequence of any possible interference detected which is associated with an eaves-

dropping, the communication established is disrupted and the key is discarded.

11. A communication system according to any one of claims 1 to 10, characterized in that the switching stations (1, 2) communicate with each other via public lines, using the encryption agreed upon.

12. A communication system according to any one of claims 1 to 11, characterized in that prior to the establishment of a communication between subscriber stations (1.1, 2.1), data transmitted from the latter to the respective switching stations (1, 2) and specific of them, such as, e.g., authentication data, are checked by the respective switching station.